Object Reuse

This module introduces the concept of object reuse, describes object reuse security ramifications and TCSEC requirements, and presents some object reuse mechanisms describing potential problem areas where object reuse errors may occur.

Module Learning Objectives

The material presented in this module can be read independently of theother modules. Upon completion of this module, the student should:

1. Understand object reuse and the security problems that can occur inthis area.
2. Understand the TCSEC object reuse requirement.
3. Be familiar with various object reuse mechanisms and their potential problem areas.

Overview

The logical concept of an object is physically implemented on a systemby resources. Typical resources include memory, disk blocks, CPU registers, and tapes. These resources are often broken down into subcomponents. Memory, for instance, may be broken into stack space, data space, execution space, file buffers, process tables, semaphores, etc. The resources that implement an object contain either object information (e.g., text, data) or authorizations to the object (e.g., MAC, DAC, privileges). The TCSEC "Object Reuse" requirement (which begins at C2 and is unchanged thereafter) is summarized as follows: when an object is formed from system resources, care must be taken to ensure that all previous information is inaccessible and all previous authorizations have been revoked before the resources are reused.

The distinction between information and authorizations is importantbecause there is some confusion in [OR92] about whether authorizations must always be revoked to satisfy the TCSEC "Object Reuse" requirement.According to Interpretation [I-0041]:

> "... [failing to clear internal data structure contents has resultedin the TCB moving] data left over from a previous subject in a TCB internal data structure to a shared object or another subject's address space. Such actions are not examples of an object reuse problem; however, they are an example of a lack of process separation or TCB isolation."

In other words, failing to clear authorizations has resulted in a process separation or TCB isolation problem. Thus, revocation (overwriting) of authorizations is always required.

When an object is deallocated (i.e., deleted), its associated resources are returned to a system "free pool." Free pools are typically used to track available resources for use at some later time. The TCSEC "System Architecture" requirement ensures that resources in a free pool are isolated fromuntrusted users. However, if resources in a free pool are not cleared before being used again, residual information and/or authorizations are exposed. Thus, when a

new object is allocated (i.e., created) from a free pool, all previous information and authorizations must be overwritten before access to the new object is granted. Since free pools are protected, this overwrite can occur eitherbefore the resources are placed in the free pool (i.e., on deallocation) or after they are released from the free pool (i.e., on allocation). In either case, it must occur before access to the new object is granted to any subject.

There are three different ways that resources can be overwritten: with a fixed pattern, with a random pattern, or with data provided by the user beforethe user is granted read access to the object. This last mechanism is referred to as "write before read," meaning that the user must overwrite the space used for the new object before the user can read it. A user cannot read back any more from the object than what the user wrote into the object.

Relevant Trusted Product Evaluation Questionnaire Questions

2.7 OBJECT REUSE

C2:

1. How is reuse of data in the storage resources (e.g., memory page cache, CPU registers, disk sectors, magnetic tapes, removable disk media, terminals) of the system prevented? (Examples include writing predefined patterns, writing random patterns, preventing reading before writing, etc.)
2. When do these actions take place: prior to allocation or after deallocation and/or release?
3. Describe the TCB (a) hardware, (b) software and (c)procedural mechanisms used to accomplish the clearing for each type of storage resource.
4. Is it possible to read data that have been "logically" deleted,but not physically removed (e.g., attempting to read past the end-of-file mark)?

Required Readings

TCSEC85 National Computer Security Center, *Department of Defense Trusted Computer Security Evaluation Criteria*, DoD 5200.28-STD, December 1985.

Sections 2.2.1.2, 3.1.1.2, 3.2.1.2, 3.3.1.2, and 4.1.1.2 contain the object reuse requirements, which are summarized on page 103.

INTERP94 National Computer Security Center, *The Interpreted TCSEC Requirements*, (quarterly).

The following Interpretations are relevant to object reuse:

I-0041 Object reuse applies to all system resources

I-0170 Functional tests required for object reuse

OR92 National Computer Security Center, *A Guide to Understanding Object Reuse in Trusted Systems*, NCSC-TG-018, Version 1, July 1992.

This document provides a description of what the TCSEC object reuse requirements mean and provides guidance on how to design and incorporate effective object reuse mechanisms into systems.

Holling76 Hollingsworth, D. and Bisbey, R. II, *Protection Errors in Operating Systems*, UCS Information Sciences Institute, Marina del Rey, CA, June 1976.

This paper provides an excellent description of what the concerns of object reuse are and describes a number of areas where potential security violations can occur during the reuse of objects.

Wichers90 Wichers, D., "Conducting an Object Reuse Study," *Proceedings of the 13th National Computer Security Conference*, pp. 738-747, October 1990.

This paper describes what the concerns of object reuse are, what the TCSEC object reuse requirements are, and then describes how an object reuse study could be conducted that would determine whether a system satisfied the TCSEC object reuse requirements.

Supplemental Readings

REMAN91 National Computer Security Center, *A Guide to Understanding Data Remanence in Automated Information Systems*, NCSC-TG-025, Version 2, September 1991.

This document provides information relating to the clearing, purging, declassification, destruction, and release of most AIS storage media.

Other Readings

None.